Privacy Notice

March 2026

This Privacy Notice explains how Vistra ("Vistra" "us", "we" and "our") collects, uses, maintains, protects, and discloses personal data from our websites or as part of our services.

'Vistra' refers to, as applicable, **Vistra ITCL (India) Limited**. Vistra is the data controller of your personal data and is subject to applicable data protection laws and regulations, which may include, but not be limited to, The Digital Personal Data Protection Act, 2024 (DPDP Act India), the EU General Data Protection Regulation 2016/679 ("GDPR"), and the Personal Data Privacy Ordinance (Chapter 486 of the laws of Hong Kong) (collectively, the "Applicable Data Protection Laws").

Please note that depending on the nature of the services we provide to you, this Privacy Notice will be supplemented with specific privacy policies and notices where required by applicable laws. Particular members of the Vistra Group may have their own Privacy Notice and may provide that directly to you, although their practices are always governed by this Privacy Notice and Vistra's internal privacy policy framework. If you are interested in the practices of a particular Vistra company, please check the "privacy" link on that Vistra company's website or contact us at privacy@vistra.com

Personal data will be collected by us only for lawful purposes and all practicable steps will be taken to ensure that personal data held by us is accurate. We shall moreover use all reasonably practicable steps to protect any personal data we hold against unauthorised or accidental access, processing, erasure, loss or use. If we engage a data processor to process any personal data held by us, we shall adopt contractual or other means to ensure that the data processor complies with our data security requirements. We shall only use personal data for the purposes for which your personal data was originally collected, for purposes compatible with those purposes, and as further detailed herein.

Vistra may update this Privacy Notice from time to time. We advise you to periodically review this Privacy Notice to be informed of how Vistra is protecting your privacy.

This Privacy Notice outlines Vistra's practices and the choices you have concerning the collection and use of your personal data. This Privacy Notice should be read together with the applicable terms and conditions, terms of engagement, or service agreements of the relevant service or website provided by Vistra (the "Terms and Conditions"). For the avoidance of doubt, nothing in this privacy notice overrides any of rights or obligations of the parties under the Terms and Conditions.

Queries and Contact Details

Requests for access, correction, complaints, or other queries relating to how your personal data is processed should be addressed to us via the contact details set out below:

By post:

Vistra ITCL (India) Limited

The Qube, 2nd floor, A wing, Hasan Pada Road, Mittal Industrial Estate, Marol, Andheri (E), Mumbai – 400059

By email:

itclcomplianceofficer@vistra.com

This Privacy Notice supersedes any previous Privacy Notice or equivalent which you may have been provided with or seen prior to the Effective Date stated above.

Your rights

Under the Applicable Data Protection Laws, you may have (any of) the following rights:

- to obtain access to, and copies of, the personal data that we hold about you;
- to require that we cease processing your personal data if the processing is causing you damage or distress;
- to require us not to send you marketing communications;
- to require us to erase your personal data;
- to require us to restrict our data processing activities;
- to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
- to require us to correct the personal data we hold about you if it is incorrect;
- to withdraw your consent at any point of time in case we were processing your personal data based on such consent;
- to lodge a complaint to us.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

You also have the right to complain to the data protection authority in your country, in event you are unhappy with how we are processing your data or how we have fulfilled your data protection request(s). To find out more about your rights, please refer to the relevant data protection governmental body or regulatory authority (as the case may be) in the place where you are located.

If you have any questions about how we use your personal data, or you wish to exercise any of the rights set out above, please contact us via any of the contact details set out under the heading "Queries and Contact Details" above.

How we collect your data

In the majority of cases, we collect personal data directly from you or from third parties. For example, we may collect your personal data from your authorised representatives and advisor(s), your employer, our corporate clients where we are providing services to them, our service providers or referees, in the case of prospective employees. We may ask you for personal data (including Contact Information and Relationship Information) when you interact with us, such as registering on our websites, signing up to receive a newsletter, or making a purchase. We may

collect additional Relationship Information from third party search information suppliers who can help us better understand our customers.

We collect transaction information when you purchase services or products from Vistra. We also collect transaction information when you visit our website, use our applications or contact us, such as for customer service purposes.

If you interact with us online, we use cookies and other technological tools to collect information about your computer and your use of our website and applications. For more information about cookies and other technologies, please see the section Cookies and Other Data Collection Technologies below.

Types of personal data collected

This Privacy Notice explains our practices with regard to "personal data" collected by Vistra for its business purposes. Personal data include any information that can be used (directly or indirectly) to identify, locate or contact you from that information alone or in combination with other information we process or can reasonably access. We may collect the following types of personal data:

- your personal identification information (which may include your name and Identity and address proof, your IP address, politically exposed person (PEP) status, personal data available in the public domain, details of your financial information, sources of wealth and your assets and such other information as may be necessary for Vistra to provide its services and to complete its client due diligence process and discharge its AML/CFT obligations).
- "Contact Information" that allows us to communicate with you, such as your name, username, mailing address, telephone numbers, email address or other addresses that allow us to send you messages.
- "Relationship Information" that helps us do business with you, such as the types of products and services that we provide to you or that may interest you, information on your company's size, geographic locations, creditworthiness and demographics.
- "Transaction Information" about how you interact with Vistra, including purchases, inquiries, customer account information, and information about how you use the Vistra websites and applications.
- if you apply for a position with us, we may collect information relating to your past employment, professional qualifications and education, your nationality and immigration/residential status, opinions from third parties about you (such as references) and other details about you which may be gathered during the recruitment process. Except where this is prohibited by applicable laws, we may also review publicly available information about you on your social media accounts.
- certain types of personal information, such as some government-issued identification numbers, biometrics or information about religion, health or sexuality, are considered sensitive and require additional protection under applicable laws. We limit the circumstances under which we may collect sensitive personal information and will seek your explicit consent where required; examples of this information include the following:

- Biometric information for identification and verification purposes
- National identification numbers may be required for identification and verification purposes.

If we ask your consent to provide personal information, we will make clear that you have the right to withdraw your consent at any time.

The basis for processing your personal data (other than with your consent), how we use that personal data and whom we share it with

I. **Performance of a contract with you**

We may process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract.

In this respect, we may use your personal data for the following:

- to prepare a proposal for you regarding the services we offer;
- to provide the services as set out in our services agreement or terms of engagement with you or as otherwise agreed with you from time to time;
- to deal with any complaints or feedback you may have;
- for any other purpose for which you provide us with your personal data in connection with a contract with you; and
- for background checks and pre-employment screenings, including conducting such checks and screenings on job applicants and employees.

II. Legitimate interests

We may also process your personal data because it is necessary for our legitimate interests, or sometimes where it is necessary for the legitimate interests of another person.

In this respect, we may use your personal data for the following:

- for marketing to you. In this respect, see the separate section on “Marketing” below;
- training our staff or monitoring their performance;
- for the administration and management of our business, including recovering money owed to us, and archiving or statistical analysis;
- to protect our rights or those of you and/or our clients and/or to prevent fraud;
- to develop and improve our services or to strengthen our relationship with you;
- for security purposes, including by operating security cameras in various locations at Vistra’s premises, and conducting background checks and pre-employment screenings;
- monitoring and recording telephone calls and emails and internet use in accordance with our IT policies;
- seeking advice on our rights and obligations, such as where we require our own legal advice; and defending, prosecuting or making a claim against you, us or a third party.

We may share your personal data with, or transfer it to, the following parties:

- your agents, advisers, intermediaries, and custodians of your assets who you tell us about;
- third parties whom we engage to assist in delivering the services to you, including other companies in the Vistra Group;
- our professional advisers where it is necessary for us to obtain their advice or assistance, including lawyers, accountants, IT or public relations advisers;
- our bankers, insurers and insurance brokers;
- other third parties such as intermediaries who we introduce to you. We will wherever possible tell you who they are before we introduce you;
- our data storage providers and any other software providers that we require to perform our services; and
- third parties and their advisers where those third parties are acquiring, or considering acquiring, all or part of our business.

III. Legal obligations

We may also process your personal data for our compliance with a legal or regulatory obligation which we are under.

In this respect, we may use your personal data for the following:

- to meet our legal, compliance and regulatory obligations, such as compliance with anti-money laundering laws;
- as required by tax authorities or any competent court or legal authority;
- monitoring and recording telephone calls and emails, and conducting background checks and pre-employment screenings for compliance with our regulatory obligations; and
- for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

We may share your personal data with the following parties:

- our advisers where it is necessary for us to obtain their advice or assistance;
- our auditors where it is necessary as part of their auditing functions;
- third parties who assist us in conducting background checks;
- other companies in the Vistra Group;
- relevant regulators or law enforcement agencies where we are required to do so.

Online Payment

If you sign up for one of our services through any of our websites or online portals that requires payment of fees using a credit card, you will be directed to another site, managed by our third-party payment processor, in order for your payment to be processed. You will be required to provide your payment details, which will be securely encrypted and handled separately by our third-party payment processor. We will not receive and/or store your payment details, but once you have made payment we will receive confirmation that your payment has been processed and with certain details regarding the transaction including the amount paid.

We currently use third-party payment processors such as Stripe for card payments. To view Stripe's Privacy Policy, please click here.

Transfer and processing of your personal data cross-border

The Vistra group of companies offer a wide range of services with business processes, management structures and technical systems that cross borders. We may transfer, store, or process your personal data in locations outside the jurisdiction in which you are based ("Jurisdiction"). Where the countries to which your personal data is transferred do not offer an equivalent level of protection for personal data to the laws of the Jurisdiction, we will ensure that appropriate and reasonable safeguards and security measures are put in place. We have designed our practices to provide a globally consistent level of protection for personal data all over the world. This means that before we transfer personal data from the Jurisdiction, we will take the necessary steps to ensure that your personal data will be given adequate protection and only transferred in accordance with the international data transfer mechanism as required by the applicable data protection laws and regulations. Intra-group transfers within Vistra companies are regulated by an intra-group data sharing agreement incorporating standard contractual clauses.

Marketing

From time to time we may send you marketing communications about similar or related services we provide, as well as other information in the form of alerts, newsletters and invitations to events or functions which we believe might be of interest to you.

We may communicate this to you in a number of ways including by post, telephone, email, SMS or other digital channels. You can unsubscribe from our communications at any time by:

- Replying STOP to the SMS to opt out
- Clicking the unsubscribe link in our emails
- Filling in form on this page https://www.vistra.com/unsubscribe
- Using the unsubscribe option in our mobile app
- Informing us during sales calls
- Contacting us through the details under "Queries and Contact Details" above.

No mobile information will be shared with third parties for marketing purposes.

We may issue service-related announcements to you when necessary (e.g. new laws, regulations or compliance requirements). You may not be able to opt out of these announcements which are service-related and not promotional in nature.

Cookie, Google Analytics and other Data Collection Technologies

When you visit our website or use our mobile applications, we collect certain Transaction Information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs and web beacons.

For example, when you visit our website, we place cookies on your computer. Cookies are small text files that websites send to your computer or other internet-connected device to uniquely identify your browser or to store information or settings in your browser. Cookies allow us to recognize you when you return. They also help us provide a customized experience and enable us to detect certain kinds of fraud. In many cases, you can manage cookie preferences and opt-out of having cookies and other data collection technologies used by adjusting the settings on your browser. All browsers are different, so visit the "help" section of your browser to learn about cookie preferences and other privacy settings that may be available.

We collect many different types of information from cookies and other technologies. For example, we may collect information from the device you use to access our website, your operating system type, browser type, domain, and other system settings, as well as the language your system uses and the country and time zone where your device is located. Our server logs also record the IP address assigned to the device you use to connect to the internet. An IP address is a unique number that devices use to identify and communicate with each other on the internet. We may also collect information about the website you were visiting before you came to Vistra and the website you visit after you leave our site.

In many cases, the information we collect using cookies and other tools is only used in a non-identifiable way, without any reference to personal data. For example, we use information we collect about all website users to optimize our websites and to understand website traffic patterns.

In some cases, we do associate the information we collect using cookies and other technology with your personal data. This Privacy Notice applies to the information when we associate it with your personal data.

For full details on how cookies are used on our website, please see our Cookie Policy.

Google Analytics

One of the third party vendor used by Vistra is Google Analytics. For information on how Google Analytics uses data please visit "How Google uses data when you use our partners' sites or apps", located at www.google.com/policies/privacy/partners/.

Use of Artificial Intelligence

We use artificial intelligence ("AI") technologies to enhance the efficiency, accuracy, and overall quality of the services we provide. AI supports the analysis and improvement of how we process, generate, and respond to queries and online forms. This includes improving information analysis, streamlining internal workflows, automating routine tasks, and enhancing the delivery and

personalisation of our services. AI is also used for quality assurance and continuous service improvement; however, it does not replace human judgment or decision-making.

When personal data is processed using AI, it is always handled in accordance with applicable data protection laws, with safeguards in place to protect your rights and interests. Any decisions that could have legal or similarly significant effects on individuals will always involve meaningful human review.

We have established a formal AI Governance Policy to ensure that our use of AI is responsible, transparent, and compliant with evolving regulations such as the EU AI Act. This includes:

- a risk-based classification framework for AI systems,
- mandatory data protection impact assessments for higher-risk use cases,
- oversight by a cross-functional AI Governance Committee, and
- regular reviews to ensure risks to individuals are identified and mitigated.

We also apply strong technical and organisational measures, such as anonymisation, encryption, and strict access controls to safeguard personal data. Our AI governance processes are fully integrated into our wider Data Protection Framework and support compliance with GDPR and other applicable global regulations.

Security of your information

Vistra has implemented an information security program that contains administrative, technical, and physical controls that are designed to safeguard your personal data. For example, we use industry-standard encryption technology to secure sensitive personal data when it is being collected and transmitted over the internet as well as firewalls, site monitoring and intrusion detection capabilities.

Please note that you should also take steps to protect yourself and your personal data, especially online. When you register at Vistra websites, choose a strong password, and do not use the same password that you use on other sites. Do not share your password with anyone else. Vistra will never ask you for your password in an unsolicited phone call or in an unsolicited e-mail. Also remember to sign out of the website and close your browser window when you have finished your work. This is to ensure that others cannot access your personal data and correspondence if others have access to your computer.

Third Party Privacy

This Privacy Notice only addresses the use and disclosure of information by Vistra. Other websites that may be accessible through any of Vistra's websites and/or client portals have their own privacy policies and data collection, use and disclosure practices. Our affiliates, suppliers and business partners have their own privacy policies too. We encourage you to familiarize yourself with the Privacy Notices provided by all third parties prior to providing them with information or taking advantage of an offer or promotion.

Forums, Community, Reviews and other Public Areas

Our websites may provide forums and other areas where you can communicate with others and publicly post information. Prior to posting in these areas, please read our Terms of Use carefully. You have no privacy rights in public postings. All the information you post will be accessible to anyone with internet access, and any personal data you include in your posting may be read, collected, and used by others. For example, if you post your email address, you may receive unsolicited messages. Please use caution when posting any personal data.

Children's privacy protection

We are committed to protecting children's privacy online.

Our websites are not intentionally designed for or directed at children under the age of 13 in the U.S. and 16 in California or EEA, and require no such information be submitted to us. Vistra will not knowingly or intentionally collect, store, use, or share, personal data of children under the age of 13 in the U.S. and 16 in California or EEA without prior documented parental or guardian consent.

If you are under the age of 13 in the U.S. and 16 in California or EEA, please do not provide any personal data, even if prompted by the website to do so. If you are under the age of 13 in the U.S. and 16 in California or EEA and you believe you have provided personal data to us, please ask your parent(s) or guardian(s) to notify us and we will delete all such personal data.

Sale of personal data

For the purposes of compliance with US State laws, please note that we do not sell (as "sell" is traditionally defined) your personally identifiable information to anyone else.

Change of purpose

We will only use personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use any personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process personal data without your knowledge or consent, in compliance with the above, where this is required or permitted by law.

Retention of your data

We will retain your personal data for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulations). We will process and store the relevant personal data for the duration of our services or for the duration of the business relationship. We may also store the data for processing in our local servers and Vistra Group databases, or use third party Cloud vendors and data processors where we have contractual security measures and reassurances of enhanced security measures in place for as long as it is necessary or required in order to fulfil legal, contractual or statutory obligations or for the establishment, exercise or defence of legal claims, and in general where there is a legitimate interest for doing so. In particular:

- where we have collected your personal data as required by anti-money laundering and counter-terrorist financing legislation, including for identification, screening and reporting, in accordance with our Data Retention Policy, we will normally retain that personal data for at least five (5) years and in most cases ten (10) years after the termination of our relationship, unless we are required to retain this information by another law or for the purposes of court proceedings;
- in the case of unsuccessful applicants who applied via Vistra's V-Connect applicant portal, unless otherwise notified to you, we will retain and use the information you provided to us for a period of 365 days from the date you last logged into your V-Connect account.

Changes to this statement

From time to time, we may update this Privacy Notice to reflect new or different privacy practices. We will place a notice online when we make material changes to this the Privacy Notice. Additionally, if the changes will materially affect the way we use or disclose previously collected personal data, we will notify you about the change by sending a notice to the primary email address associated with your account.

****